REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application are obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

I. REJECTION OF CLAIMS 1-11 UNDER 35 U.S.C. § 103

The Examiner has rejected claims 1-11 in the Office Action under 35 U.S.C. § 103 as being obvious over Sherer, et al. (US Patent 6,115,376, issued September 5, 2000, hereinafter referred to as "Sherer") in view of Jones, et al. (US Patent 5,623,637, issued April 22, 1997, hereinafter referred to as "Jones"). The Applicants respectfully traverse the rejection.

Sherer teaches medium access control address authentication. A network interface card on an end station used in accordance with the invention is disclosed. (See Sherer, col. 5, ll. 32-67.) Notably, the network interface card contains only a single memory module 46. (See *Id.*, emphasis added.)

Jones teaches an encrypted data storage card including smartcard integrated circuit for storing an access password and encryption keys. A user in possession of the card enters a password stored in the card's memory. (See Jones, col. 8, ll. 47-67.) If the password is correct, the user has access to needed access codes stored in the password-protected card. (See Jones, col. 9, ll. 1-21.)

The Examiner's attention is directed to the fact that Sherer and Jones, alone or in any permissible combination, fail to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Applicants' independent claims 1 and 10. Specifically, Applicants' independent claims 1 and 10 recite:

> 1. A security mechanism for enabling a user to commence a session between a network peripheral device and a network, comprising:
> an immutable memory element that contains first information including

application software that initiates and provides security services;

a persistent memory element that contains second information to enable the security mechanism to configure the network peripheral device to access different networks;

a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session; and

a tamper-evident enclosure for enclosing the memory elements. (Emphasis Added)

10. A method for facilitating a secure connection session with a user between a network peripheral device and a network, comprising the steps of:

accessing an immutable memory element that contains first information that provides security services;

accessing a persistent memory element that contains second information including configuration information to enable the security mechanism to configure the network peripheral device to access a network;

accessing a volatile memory element that contains third information, including the critical data for authentication; and

erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions. (Emphasis Added)

Applicants' invention teaches the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session. Applicants' invention advantageously allows a device to be configured to access any network and the corresponding network's software (see Applicants' Specification, para. [0006]; para. [0013]). In other words, the same laptop, for example, can be connected to various networks. Once the session is completed all of the information in the volatile memory element is erased, thereby preventing re-use of such information by unauthorized users. (See Applicants' Specification, para. [0006].)

The alleged combination (as taught by Sherer) fails to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a immutable memory element, a persistent memory element and a volatile memory element that contains third

information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Applicants' independent claims 1 and 10. First, unlike the Applicants' invention that teaches three separate types of memory elements (i.e. immutable memory element, persistent memory element and volatile memory element), Sherer only teaches that the network interface card contains a single memory element 46. (See Sherer, col 5, ll. 32-67, FIG. 3, emphasis added.)

However, the Examiner asserts in the Final Office Action, that the number of memory modules does not determine patentability. (See Final Office Action, p. 2, ll. 6-13.) Moreover, the Examiner alleges that such limitation would have been obvious because Sherer does explicitly show a program memory module subdivided into multiple segments or modules in FIG. 3. (See *Id.*) However, the Applicants' argument, as clarified, is that using three different types of memory elements is clearly patentable and not obvious. For example, it is the Applicants' novel combination of using three different types of memory elements that contributes to the Applicants' novel method for facilitating a secure connection session with a user between a network peripheral device and a network. As discussed above, this allows all of the information in the volatile memory element to be erased, thereby preventing re-use of such information by unauthorized users. (See Applicants' Specification, para. [0006].)

Moreover, as conceded by the Examiner, Sherer fails to teach or to suggest a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session. (See Office Action, p. 3, ll. 6-7.) However, the Examiner alleges that Jones bridges the substantial gap left by Sherer.

The Applicants respectfully submit that Jones fails to bridge the substantial gap left by Sherer because Jones also fails to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Applicants' independent claims 1 and 10. In fact, Jones teaches away from

the Applicants' invention because Jones clearly teaches that critical information is stored in the card's memory and fails to teach that this information is erased from the volatile memory at the completion of each connection session. (See Jones, col. 8, ll. 47-67; col. 9, ll. 1-21.) Jones specifically teaches that a user supplies a secret password that is written into the smart card I.C. memory. (See Jones, col. 8, ll. 6-9, emphasis added.) Jones further teaches that ". . . whose processor (i.e. the smart card) is programmed to combine the random number 303 at 325 with the previously stored secret password 301 to form a result value at 327." (See Jones, col. 8, ll. 21-24, emphasis added.)

Furthermore, the Examiner conceded that Sherer does not expressly disclose third information erased from the volatile memory at the completion of each session. The Examiner then alleged that Sherer suggests using different authentication schemes. Finally, the Examiner then leaps from this alleged suggestion of using different authentication schemes to make obvious the teaching of deleting session keys after the completion of a session. It is respectfully submitted that a general statement such as "using different authentication schemes" would not suggest erasing said third information from the volatile memory at the completion of each connection session. The Examiner provided absolutely no support in the alleged combination of Sherer and Jones for this teaching. In fact, the Examiner is simply using impermissible hindsight.

In rebuttal, the Examiner asserts in the Final Office Action that the Applicants' arguments with respect the limitation of "erasing the information from the volatile memory at the completion of the session" ignores the fact that one-time passwords were conventional and well known by vaguely citing to Sherer in columns 5-6. (See Final Office Action, p. 2, ll. 14-20.) However, in doing so, the Examiner contradicts his own concession that Sherer does not expressly disclose such limitation. (See *Id.* at p. 4, ll. 1-2.)

Regardless, Sherer does not support the Examiner's assertion or interpretation that one-time passwords make obvious the feature of erasing the third information (including critical data for authentication) form the volatile memory at the completion of the session. Sherer explicitly teaches storing critical data for authentication. (See Sherer, col. 5, ll. 62-67.) Sherer states "[i]n a preferred embodiment, the end station is

prevented from reading the secret value stored in the network interface cards, such as by storing it in memory location that is not within the host system address space . . ." (See *Id.*, emphasis added.) In addition, Sherer actually teaches away from the Applicants' invention because Sherer explicitly teaches that the critical data for authentication, such as private key 52, is not contained in a volatile memory element, such as RAM 46. Therefore, Sherer and Jones, alone or in any permissible combination clearly fail to teach or suggest at least the limitation of a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Applicants' independent claims 1 and 10.

In rejecting claims under 35 U.S.C. §103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. See In re Fine, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In so doing, the Examiner is expected to make the factual determinations set forth in Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed. Cir.), cert. denied, 488 U.S. 825 (1988); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281 293, 227 USPQ 657, 664 (Fed. Cir. 1985), cert. Denied, 475 U.S. 1017 (1986); ACS Hosp. Sys., Inc. v. Montefiore Hosp. 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). These showings by the Examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). It is respectfully submitted that the Examiner failed to present a prima facie case of obviousness. Therefore, the combination of Sherer and Jones clearly fails to render obvious Applicants' invention as recited in independent claims 1 and 10.

Furthermore, Applicants **again affirmatively traverse** the Examiner's use of Official Notice. It is respectfully submitted that the Examiner provides the necessary

support for the use of Official Notice. Applicants specifically challenge the Examiner's assertion that the Examiner's taking of Official Notice is now admitted prior art.

Moreover, dependent claims 2-9 and 11 depend, either directly or indirectly, from independent claims 1 and 10, respectively, and recite additional limitations. As such, and for the exact same reason set forth above, the Applicants submit that claims 2-9 and 11 are also not obvious over Sherer in view of Jones. As such, the Applicants respectfully request the rejection be withdrawn.

Conclusion

Thus, the Applicants submit that all of these claims now fully satisfy the requirements of 35 U.S.C. § 103. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the present final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

April 18, 2007

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404